Volume 15, Issue 8 • August 2020

Monthly Security Tips Newsletter

From the desk of
Michael Aliperti

MS-ISAC Chair

Working Remotely: How to be Safe, Secure, and Successful

Between working at the office, or school, or remotely, the principles of security can become something of a moving target. For some, this creates an uncertainty with making sure that the right policies are applied. Reducing risk on at-home networks, keeping information secure during virtual meetings and having a strong password policy are some best practices that can be implemented quickly and effectively from wherever you are working.

Reducing Risk on Home Networks

Home IT devices, such as unsecured off-site routers, modems, and other network devices are subject to many of the same threats as on-site business devices. They can be attacked from any device on the internet. Remote devices are also vulnerable to unauthorized access from neighbors and passersby.

As we continue to work, attend school, and connect with friends and family remotely, there are steps you can take to reduce the risk and improve the security of home networks. Consider the following list to gauge the amount of risk involved and improve the security of your home network:

- Are your network devices physically secured?
- Have you changed the default manufacturer/administrative account password on your network devices (modem and router)? Many routers will come preconfigured with a password. The default password for most router models are easily accessible on the internet, making it extremely important to change the administrative passwords and not use the default.
- Do you have a unique password and two-factor authentication (2FA) enabled on your network devices (modem and router)?
- Do you have a password policy in place? Do you have a unique password and 2FA enabled on your internet service provider's web portal?
- If you use a mobile application for network management, do you have a unique password and 2FA enabled?
- Have you installed the latest updates for your network devices (i.e., modem, router, laptop/PC) or have you enabled auto-update with the device's administration page?

- Does your network device (router/modem) support Wi-Fi Protected Access Version 2 (WPA2) or Wi-Fi Protected Access Version 3 (WPA3)? WPA2 should be the minimum.
- Have you turned off/disabled Wireless Protected Setup (WPS) and Universal Plug and Play (UPnP) on your network? If enabled, these might allow attackers to connect to your devices without permission.
- Have you changed the Wi-Fi network name to something unique that doesn't provide any identifying information?
- Have you enabled firewall on your network devices?
- Have you disabled remote management? Most routers offer the option to view and modify their settings over the internet. Turn this feature off to guard against unauthorized individuals accessing and changing your router's configuration.
- Have you hardened your device by removing ports, software or services that are unused or unwanted?
- Do you run updated antivirus and malware protection on your device?

Security during virtual meetings

In order to help protect you and your organization from potential threats, here are some cybersecurity tips on how to securely configure your virtual meetings, whether they be for work or your classroom experience:

Sharing of your information assets during virtual meetings

- Avoid adding your meeting to any public calendars or posting it on social media
- Require participants to enter an access code
- Avoid reusing access codes or meeting pins
- Distribute the meeting link and access code directly to the intended participants
- Remind invited guests not to share the access code
- Before sharing your screen, close unused windows to ensure you do not share sensitive or confidential information
- Use a privacy shield or cover over your webcam when it is not in use

Managing your information assets and password policy

- Use your organization's provided services and devices
- Do not record the meeting unless it is necessary and be aware that others may be able to record the meeting
- Disable the "Anyone Can Share" feature to prevent unauthorized screen sharing
- Muting users on entry can prevent potential disruptions
- Prevent users from sharing video by default; allow video sharing only when necessary
- Validate the participant list against invited attendees, or have participants identify themselves as they join the meeting
- Do not trust the safety of links shared in meeting chats

- Schedule “Unlisted” meetings and hide specific details, such as its host, topic, and starting time
- Do not allow attendees to “Join Before Host”
- Set up each meeting to require all attendees to enter a password
- Create a unique password comprised of upper, lower case, numbers, and special characters for each meeting
- Exclude the meeting password from attendee email invitations. Provide the password to attendees via a separate email or by phone
- On reoccurring meetings, always check to ensure one-time attendees are not included in subsequent meetings or meeting chat threads.
- Do not list personal information, such as location, phone number, or date of birth on your Skype profile

Remember, just like you protect your physical assets (shed, kayak, or bike) with a padlock, you need to lock down connectivity devices to protect information assets! A resilient cybersecurity mindset contributes towards being able to have a clear view of the objectives. For some, end points might have become a primary concern, for others, the corporate assets might have become even more susceptible in light of the increased amounts of ransomware. This dual pronged problem especially became more evident during this new world of COVID-19 with more staff working remotely.

Have you identified more risk than you initially realized? More information and mitigation techniques can be found at Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) site **https://us-cert.cisa.gov/ncas/tips/ST15-002**

Additional Resources

CIS Password Policy Guide

MS-ISAC
Multi-State Information
Sharing & Analysis Center

STOP | THINK
CONNECT

The information provided in the MS-ISAC Monthly Security Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.